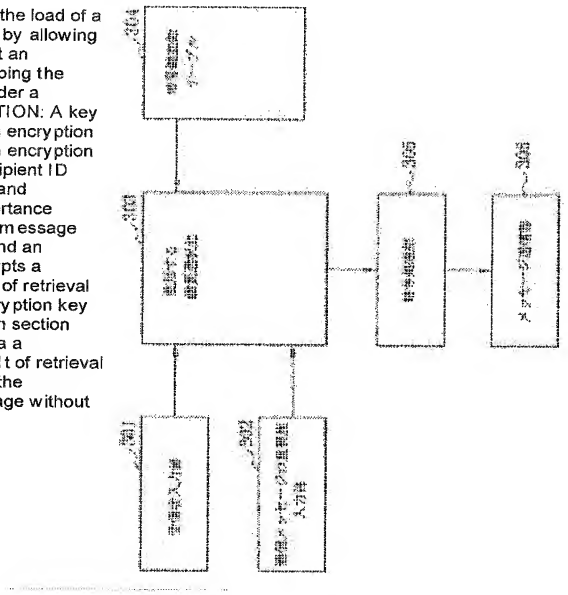
CIPHER COMMUNICATION METHOD AND STORAGE MEDIUM RECORDING ITS PROGRAM

Publication number: JP2000278260 (A)
Publication date: 2000-10-06
Inventor(s): ITO MASARU
Applicant(s): HITACHI INFORMATION SYS LTD
Classification:
- international: ***G06F13/00; H04L9/14; H04L29/08;*** **G06F13/00; H04L9/14; H04L29/08;** (IPC1-7): H04L9/14; G06F13/00; H04L29/08
- European:
Application number: JP19990079871 19990324
Priority number(s): JP19990079871 19990324

Abstract of **JP 2000278260 (A)**

PROBLEM TO BE SOLVED: To relieve the load of a sender and to save computer resources by allowing a user of cipher communication to select an optimum encryption algorithm while keeping the security of the cipher communication under a network computing environment. SOLUTION: A key length selection section 303 retrieves an encryption algorithm and an encryption key from an encryption key registration table 304 by using a recipient ID entered to a recipient entry section 301 and converted into a network class and importance information entered to a communication message importance entry section 302 as keys, and an encryption processing section 305 encrypts a message by using them when the result of retrieval shows the encryption algorithm and encryption key are existent and a message transmission section 306 transmits the encrypted message via a communication channel.; When the result of retrieval shows they are not existent in the table, the message is transmitted as a plain message without being encrypted.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2000－278260
（P2000－278260A）
(43)公開日　平成12年10月６日(2000.10.6)

(51)Int.Cl.[7]	識別記号	Ｆ Ｉ		テーマコード（参考）
Ｈ０４Ｌ　9/14		Ｈ０４Ｌ　9/00	６４１	５Ｂ０８９
Ｇ０６Ｆ　13/00	３５１	Ｇ０６Ｆ　13/00	３５１Ｚ	５Ｊ１０４
Ｈ０４Ｌ　29/08		Ｈ０４Ｌ　13/00	３０７Ｚ	５Ｋ０３４

審査請求　未請求　請求項の数４　ＯＬ　（全７頁）

(21)出願番号　特願平11－79871

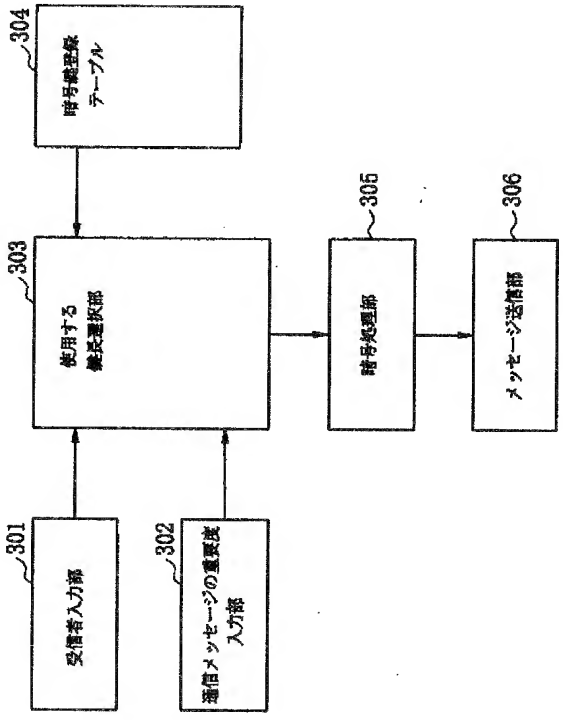
(22)出願日　平成11年３月24日(1999.3.24)

(71)出願人　000152985
株式会社日立情報システムズ
東京都渋谷区道玄坂１丁目16番５号
(72)発明者　伊藤　優
東京都渋谷区道玄坂一丁目16番５号　株式会社日立情報システムズ内
(74)代理人　100077274
弁理士　磯村　雅俊　（外１名）

Ｆターム(参考)　5B089 GA21 GB04 HA10 JA03 JA08 JA31 JB22 KA05 KA06 KB06 KB13 KC53 KH30
5J104 AA01 AA35 NA02 NA37 PA07
5K034 AA05 AA07 AA10 BB06 CC01 HH01 HH14 HH16 HH63

(54)【発明の名称】　暗号通信方法およびそのプログラムを記録した記録媒体

(57)【要約】
【課題】ネットワークコンピューティング環境下で、暗号通信の利用者は暗号通信の安全性を確保しながら、最適な暗号アルゴリズムを選択し、送信者の負担を軽減しコンピュータ資源の節約を図る。
【解決手段】受信者入力部３０１に入力された受信者ＩＤをネットワーク種別に変換し、かつ通信メッセージの重要度入力部３０２に入力された重要度とをキーとして、鍵長選択部３０３は暗号鍵登録テーブル３０４から暗号アルゴリズムと暗号鍵を検索し、検索の結果が有れば、暗号処理部３０５でそれらを用いて暗号化し、メッセージ送信部３０６から通信回線を介して暗号メッセージ送信する。検索の結果、テーブルに該当するものがなければ、暗号化せずに平文で送信する。



1

【特許請求の範囲】

【請求項１】　コンピュータネットワーク上で暗号メッセージ通信を行うメッセージ通信方法において、

暗号通信メッセージの受信者名が入力されると、該受信者名に基づき使用されるネットワークの種別を算出し、

通信メッセージの秘匿の必要性の段階が入力されると、該ネットワークの種別およびメッセージの秘匿の必要性の段階をキーとして、暗号鍵登録テーブル中から使用すべき暗号アルゴリズムと暗号鍵を検索し、

検索の結果、該当する暗号アルゴリズムと暗号鍵が存在すれば、該暗号アルゴリズムと暗号鍵でメッセージを暗号化し、

暗号されたメッセージを送信することを特徴とする暗号通信方法。

【請求項２】　前記暗号鍵登録テーブルには、ネットワークの種別とメッセージ重要度に対応して、暗号アルゴリズムと暗号鍵が登録されていることを特徴とする請求項１に記載の暗号通信方法。

【請求項３】　前記暗号通信メッセージの受信者名が入力されると、受信者名とＩＰアドレスとがマッピングされたデータベースにより、該当するＩＰアドレスが抽出され、該当ＩＰアドレスより使用される通信回線が判別されることを特徴とする請求項１に記載の暗号通信方法。

【請求項４】　請求項１～３のうちのいずれかに記載の暗号通信方法の処理をプログラムに変換し、変換されたプログラムを記録したことを特徴とする記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ネットワークコンピューティング環境で、暗号メッセージ通信を行うメッセージ通信方法およびそのプログラムを記録した記録媒体に関し、特に種々のネットワークを使用し、かつ通信メッセージの重要性に応じて必要な暗号アルゴリズムと必要な長さの暗号鍵を選択して送信することができるので、必要な強度の暗号文が得られるとともに、暗号化に伴う費用を低減することができる暗号通信方法およびそのプログラムを記録した記録媒体に関する。

【０００２】

【従来の技術】ネットワークコンピューティング環境下で暗号メッセージ通信を行う場合、秘密鍵暗号（慣用暗号）を用いる第１の方法と公開鍵暗号を用いる第２の方法がある。秘密鍵暗号を使用する場合には、送信者と受信者が予め定められた同一の暗号鍵を保有しておき、送信者は当該暗号鍵で平文を暗号化し、受信者は当該暗号鍵で暗号文を平文に復号化する。この場合、通信に先立って送信者と受信者間で同一の暗号鍵を第３者に知れること無く、安全に保有することが課題となる。従って、第１の方法では、身近な人相互間の通信、相手が判っている人との間での通信に適している。他方、公開鍵暗号

2

を使用する場合には、予め、暗号通信の利用者ごとに暗号鍵（公開鍵）と復号鍵（秘密鍵）を生成しておき、送信者は受信者の暗号鍵で平文を暗号化し、受信者は自分の復号鍵で暗号文を平文に復号化する。したがって、暗号鍵は暗号通信の不特定多数の利用者に開示され、復号鍵は、特定の１人の利用者（メッセージ受信者）のみに知らせることが必要であるが、秘密鍵暗号の前述の課題である同一の暗号鍵を送受信者間で事前に保有する必要はない。従って、第２の方法では、知らない相手方との間の通信、電子取引による通信等に適している。

【０００３】ここで、暗号鍵と復号鍵は数学的関数関係を有し、暗号鍵から復号鍵を特定することが計算量的に困難であることが前提となる。例えば、代表的なRSA暗号においては、50桁以上の素数ｐ、ｑを選択し、ｎ＝ｐ×ｑを求め、復号鍵eを（ｐ－１）×（ｑ－１）と互いに素な整数に設定する。そして、ｄをe×d=1mod（（q－１）×（ｐ－１））として求め、ｎとｄを暗号鍵とする。これにより、復号鍵eを特定することは、ｎからｐとｑを算出することに帰着されるため、50桁以上の素数の素因数分解と同値の計算量的困難性を得る。また、秘密鍵暗号は、コンピュータシステム内に記録された情報に対して、ビット単位の変換処理を特定の量で一括して行い、公開鍵暗号は、コンピュータシステムに記録された情報を数値量とみなして、数学的関数変換を行うため、秘密鍵暗号は、公開鍵暗号に比べて、極めて高速に動作し、消費するコンピュータ資源（メモリ、CPU）は少量ですむ。

【０００４】さらに、秘密鍵暗号、公開鍵暗号とも暗号文の解読の困難性は、暗号鍵の長さに依存する。例えば、秘密鍵暗号の代表的なDES暗号では、暗号鍵のビットパターンを元に、平文のビットパターンを攪拌し、排他的論理和を取り暗号文を作成する。RSA暗号では、前述のように選択する素数ｐとｑの桁数が多いほど、すなわち公開鍵ｎ、ｄの桁数が多いほど、秘密鍵の算出が困難になる。そこで、秘密鍵暗号や公開鍵暗号を用いた暗号メッセージ通信では、暗号鍵の長さが長いほど、指数関数的に解読が困難になってくるが、他方暗号化、復号化に必要なコンピュータ資源（CPU、メモリ）と処理時間が指数関数的に多くなる。ところで、従来、取引毎に使用する暗号化方法を変化させ、また暗号化キーデータを不規則に変動させることにより、第３者による電文の暗号化データの解読を困難にすることを目的とした電文暗号化方式が提案されている（例えば、特開平１０－１０５６２４号公報参照）。この方法では、利用者が電文の暗号化方法として、例えば銀行と顧客間で残高照会内容を送受信する場合には、暗号化パターン１を選択し、磁気カード上の口座番号とパターン１の暗号化キーデータの排他的論理和をとり、暗号化口座番号を作成している。しかしながら、上記公報に記載の暗号化方法では、何の根拠もなく、種々のパターンから１つを自由に選択

するものであって、その通信に真に必要な強度の暗号文が得られるかは不明であり、また暗号化に伴う費用も低減できるか否かは不明である。

【０００５】

【発明が解決しようとする課題】上述のように、ネットワークコンピューティング環境で、暗号メッセージ通信を行う場合、暗号アルゴリズムや暗号鍵長の選択は、利用者の利便性やコンピュータ経費に大きく影響するため、必要な秘匿性の程度や使い勝手、費用を考慮して選択する必要がある。すなわち、暗号メッセージに必要な解読の困難性の程度は、使用するネットワークの特性やメッセージの内容に依存する場合が多い。例えば、インターネットや無線を使用したメッセージ通信では、通信経路上の暗号メッセージが不特定多数の人にアクセス可能になるため、一般に必要な解読の困難性が高い。他方、専用通信回線を使用したメッセージ通信では、通信経路上の暗号メッセージにアクセス可能な人が特定される為、必要な解読の困難性は相対的に低い。さらに、利用者の立場では、通信メッセージの重要度に応じて必要な解読の困難性が変化することは、言うまでもない。

【０００６】また、前述のように、秘密鍵暗号は公開鍵暗号に比べて高速であり、所要コンピュータ資源も少量であるが、送受信者間で暗号鍵を安全に共有する困難さがあるため、一般に特定グループの人が使用するネットワークの場合（例えば、企業内ネットワーク）には適するが、インターネットなどの不特定の人が使用するネットワークには、公開鍵暗号が適している。しかし、近年のように、ネットワークコンピューティング環境が普及している状況下では、コンピュータシステムからのアクセス可能なネットワークが増加し、メッセージ送信先も多岐に渡っているため、利用者が上記のような暗号アルゴリズムや暗号鍵長を考慮し、多数の種類の中から１つを選択して、それを用いて暗号メッセージ通信を行うことは困難になってきている。

【０００７】そこで、本発明の目的は、従来の暗号メッセージ通信における上述のような問題点を解消し、コンピュータネットワーク上で、暗号メッセージ通信を行う場合に、メッセージの暗号化処理に先立って、使用するネットワークの状況や通信メッセージの内容によって、必要な強度の暗号文が得られ、かつ暗号化に伴う費用を低減できるような暗号通信方法とそのプログラムを記録した記録媒体を提供することにある。

【０００８】

【課題を解決するための手段】上記目的を達成するため、本発明の暗号通信方法では、利用者が暗号化処理を行う度毎に、送信先と通信メッセージの秘匿の必要性を、利用者に比較的簡明な情報で指定することにより、使用するネットワークの種類を判別し、暗号アルゴリズムと暗号鍵を選択できるようにして、ネットワークの種類や通信メッセージの内容に適した強度の暗号化方法を

与える。そのために、受信者名を入力することにより、ＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）アドレスに変換するようにマッピングしておき、変換されたＩＰアドレスから使用するネットワークの状況を判別し、またメッセージの重要度を入力することにより、必要な強度の暗号文が得られるように、自動的に最適の暗号アルゴリズムと暗号鍵が選択されるようなテーブルを作成しておく。次に、選択された暗号化アルゴリズムと暗号鍵を用いてメッセージを暗号化し、暗号文の送信および受信を行う。これにより、利用者は容易に暗号通信の安全性を確保しながら、最適な暗号アルゴリズムと必要な長さの暗号鍵を選択することができるので、送信者の負担の軽減とコンピュータ資源の節約を図ることができる。

【０００９】

【発明の実施の形態】以下、本発明の実施例を、図面により詳細に説明する。図１は、本発明が適用される通信システムの全体概要図である。図１において、１０１は送信者用コンピュータ、１０２は狭域ネットワークであるLAN（Local Area Network）、１０３はLAN１０２を介して送信者用コンピュータ１０１からメッセージを受信する受信者A用コンピュータ、１０４は遠隔地へのメッセージ送信を行い、特定のコンピュータのみが使用可能な専用回線、１０５は、専用回線１０４を介してコンピュータ１０１からメッセージを受信する受信者B用コンピュータ、１０６は遠隔地へのメッセージ送信を行い、不特定のコンピュータから使用可能な公衆回線、１０７は公衆回線１０６を介してコンピュータ１０１からメッセージを受信する受信者C用コンピュータ、１０８は電波によりメッセージ送信を行う無線設備、１０９は無線設備１０８を介してコンピュータ１０１からメッセージを受信する受信者D用コンピュータ、１１０は常時不特定のコンピュータが使用し、経路が不特定なインターネット、１１１は、インターネット１１０を介して、コンピュータ１０１からメッセージを受信する受信者E用コンピュータ、１１２はLAN１０２から専用回線１０４、インターネット１１０、公衆回線１０６および無線設備１０８へのルートを選択して送信するルータ、１１３，１１４，１１５も受信者B,C,D用コンピュータ１０５，１０７，１０９にそれぞれルートを選択して送信するルータである。

【００１０】図２は、本発明の一実施例を示す通信メッセージの重要度に応じた内容例のテーブルの図である。図２において、２０１は通信メッセージの暗号文に対して必要となる解読の困難性を３段階（大、中、小）に区分した項目、２０２は項目２０１の各段階に該当するメッセージの例である。このテーブルは、送信者用コンピュータ１０１は勿論のこと、受信者B,C,D,E用コンピュータ１０５，１０７，１０９，１１１の各メモリに格納されている。受信者用コンピュータも、次回には送信用コンピュータになる可能性を有している。これ例では、

電子決済用のクレジットカード番号や、個人のプライバシー情報を含んだメッセージに対しては解読の困難性が大のものが必要であり、社内の売上げデータを記述したメッセージに対しては、解読の困難性が中程度のものが必要であり、会議案内のようなメッセージは解読の困難性が小のものでよいことが判別される。

【００１１】図３は、図１における送信者用コンピュータ内の処理装置のブロック図である。送信者用コンピュータ１０１で実行される処理装置は、図３に示すような構成となっている。図３において、３０１は送信者が受信者名（受信者ID)を入力する処理部、３０２は送信者が通信メッセージに対して必要となる解読の困難性の段階を入力する処理部、３０３は受信者入力部３０１と重要度入力部３０２から入力されたデータをもとに使用する暗号鍵を選択する処理部、３０４は受信者に対応して、すなわち使用するネットワークの種類と必要な解読の困難性の段階に対応して、選択すべき暗号鍵を登録した暗号鍵登録テーブル、３０５は鍵長選択部３０３で選択した暗号鍵にもとずき通信メッセージを暗号化する処理部、３０６は暗号化処理部３０５で暗号化した通信メッセージを送信する処理部である。受信者入力部３０１の入力と通信メッセージの重要度入力部３０２の入力とを同時に行うか、あるいはシリアルに行うかは任意に決められるが、ここでは、同一画面でほぼ同時に入力された両方の入力データを、入力部３０１および３０２にそれぞれ入力して処理する。

【００１２】受信者入力部３０１では、受信者IDが入力されることにより、ＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）アドレスに変換するようにマッピングされたデータベースが配置されており、変換されたＩＰアドレスから使用するネットワークの状況を判別して、受信者がＬＡＮ１０２に接続されているか、インターネット１１０に接続されているか、専用回線１０４に接続されているか、公衆回線１０６に接続されているか、あるいは無線回線１０８に接続されているかを判別し、判別した情報を鍵長選択部３０３に送る。例えば、ＩＰアドレスの先頭部分の何ビットを判別範囲にしておき、その部分が異なればインターネット、あるいは遠距離回線であると判別する。先頭部分が送信者のＩＰアドレスと同じであれば、ＬＡＮであると判別する。一方、メッセージ重要度入力部３０２では、クレジットカード、プライバシー情報、社内の売上げデータ、社内の会議録、会議案内等の内容が入力されることにより、図２に示すテーブルを検索して必要な解読の困難性の段階を自動的に得る。得られた必要性の段階は、鍵長選択部３０３に送られる。

【００１３】図４は、図３で示した処理ブロック図における暗号鍵登録テーブルの概念図である。図４において、４０１は使用するネットワーク種別を示す項目、４０２は通信メッセージに必要になる暗号文の解読困難性の程度を示す項目、４０３はネットワーク種別４０１、メッセージ重要度４０２の項目に対応して使用する暗号アルゴリズムの項目、４０４は４０１、４０２、４０３の項目に対応した暗号鍵長（ビット数）、４０５は使用する暗号鍵である。なお、暗号アルゴリズム４０３において、Ｄｅｓは暗号鍵

図４に示すように、自動的に最適の暗号アルゴリズムと暗号鍵が選択されるようなテーブルを作成しておくことにより、鍵長選択部３０３は入力されたネットワークの種別とメッセージの重要度に基づいて、このテーブルから暗号化アルゴリズム４０３と暗号鍵４０５とを自動的に選択する。そして、これらを暗号処理部３０５に送る。暗号処理部３０５では、送られた暗号化アルゴリズム４０３と暗号鍵４０５を用いてメッセージを暗号化し、メッセージ送信部３０６に送る。メッセージ送信部３０６では、送られた暗号文にヘッダ等の制御文を付加し、各回線に適合した制御を行うことにより暗号メッセージを送信する。

【００１４】図５は、本発明の一実施例を示す暗号通信方法の動作フローチャートである。図５において、ステップ５０１は暗号通信メッセージの受信者名を送信者が入力する処理、ステップ５０２はステップ５０１で入力した暗号メッセージの受信者名に基づき、使用されるネットワークの種別を算出する処理、ステップ５０３は通信メッセージの内容に基づき、送信者が秘匿の必要性の段階を入力する処理、ステップ５０４はステップ５０２で求めたネットワークの種別とステップ５０３で入力された通信メッセージの必要な秘匿性の程度をキーとして、暗号鍵登録テーブルの中から、使用すべき暗号アルゴリズムと暗号鍵を検索する処理、ステップ５０５は検索処理ステップ５０４の結果、一致する暗号アルゴリズムと暗号鍵が暗号鍵登録テーブル中に存在したか否かを判定する判定処理、ステップ５０６は通信メッセージの平文を暗号化する処理、ステップ５０７は暗号文を送信する処理、ステップ５０８は平文を送信する処理である。

【００１５】次に、図５を用いて、本発明の動作を説明する。先ず、送信者用コンピュータ上から送信者が受信者IDを入力する（ステップ５０１）。次に、受信者IDをIPアドレスなどに変換することにより、使用するネットワークの経路、種別を算出する（ステップ５０２）。次に、送信者用コンピュータ上から、送信者は、メッセージの重要度に応じて必要な秘匿性の程度を'大'、'中'、'小'の三段階から選択して入力する（ステップ５０３）。これにより、図４の暗号鍵登録テーブルを検索する（ステップ５０４）。暗号鍵登録テーブルの検索結果を判定し（ステップ５０５）、ステップ５０２で算出したネットワーク種別、ステップ５０３で入力した必要な秘匿性の程度に該当する暗号アルゴリズムと暗号鍵が登録されていない場合には、通信メッセージを平文で送

信する（ステップ５０８）。他方、暗号鍵登録テーブルの検索結果判定により（ステップ５０５）、該当する暗号アルゴリズムと暗号鍵が登録されている場合は、当該アルゴリズムと暗号鍵でメッセージを暗号化し（ステップ５０６）、当該暗号文を送信する（ステップ５０７）。

【００１６】このように、本実施例においては、利用者は受信者ID情報と通信メッセージの重要性を指定すれば、暗号メッセージに対して、必要な秘匿性を確保しつつ、コンピュータ消費資源が少なく、使い勝手の良い暗号を利用することができる。また、前述のように、本発明に係わる暗号化手順を選択する処理ステップをコンピュータプログラムで実現する場合、このプログラムをCD-ROM等の記録媒体に記録した形態で、商品として流通させることが可能である。また、この記録媒体を任意の場所に設置されたパーソナルコンピュータに挿入して、プログラムをインストールすることにより、あるいは通信回線を介して他のコンピュータから転送してインストールすることにより、任意の時刻に本発明を実現して、必要な暗号鍵とアルゴリズムを自動選択して暗号メッセージ送信することができる。

【００１７】

【発明の効果】以上説明したように、本発明によれば、ネットワークコンピューティング環境が下において、暗号通信の利用者は、容易に暗号通信の安全性を確保しつつ、最適な暗号アルゴリズムを選択可能になるため、送信者の負担軽減やコンピュータ資源の節減が図れる。さらに、通信メッセージの重要度に応じて暗号アルゴリズムと必要な長さの暗号鍵が選択できるため、全体的に暗号通信の安全性が高まるという効果がある。

【図面の簡単な説明】

【図１】本発明が適用される通信システムの全体概要図である。

【図２】本発明の一実施例を示す通信メッセージの重要度に応じた内容例のテーブル図である。

【図３】図１における送信者用コンピュータに内蔵された処理ブロック図である。

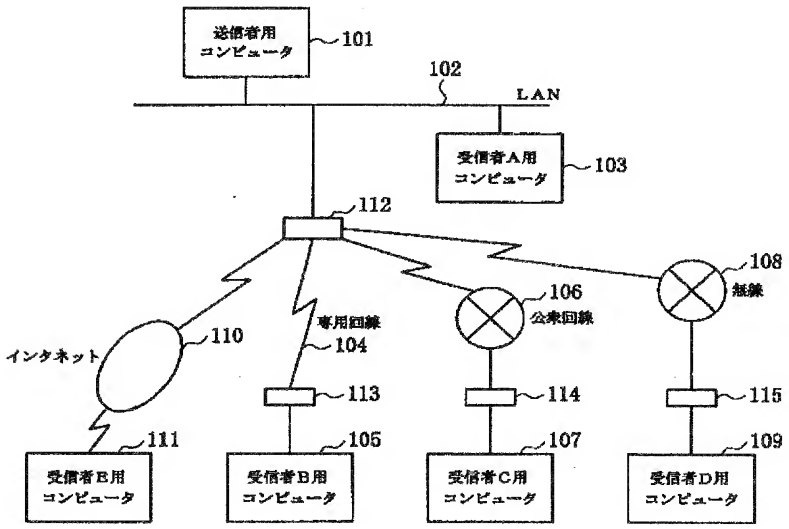
【図４】図３における暗号鍵登録テーブルのフォーマット図である。

【図５】本発明の一実施例を示す暗号通信方法の動作フローチャートである。

【符号の説明】

１０１…送信者用コンピュータ、１０２…LAN（Local Area Network）、１０３…受信者A用コンピュータ、１０４…専用回線、１０５…受信者B用コンピュータ、１０６…公衆回線、１０７…受信者C用コンピュータ、１０８…無線設備、１０９…受信者D用コンピュータ、１１０…インターネット、１１１…受信者E用コンピュータ、１１２～１１５…ルータ、２０１…必要な解読の困難性の段階の欄、２０２…段階に対するメッセージ、３０１…受信者ID入力部、３０２…メッセージ重要度入力部、３０３…鍵長選択部、３０４…暗号鍵登録テーブル、３０５…暗号処理部、３０６…メッセージ送信部、４０１…ネットワーク種別、４０２…メッセージ重要度、４０３…暗号アルゴリズム、４０４…鍵長、４０５…暗号鍵。

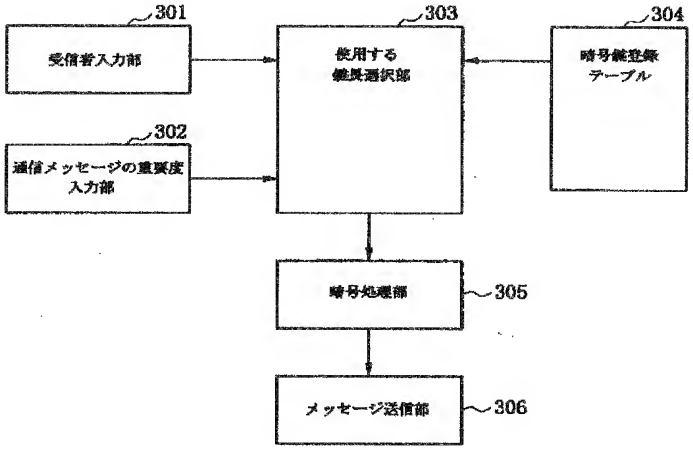
【図１】



【図２】

201 必要な解読の困難性	202 メッセージの例
大	・電子決済用のクレジットカード番号 ・個人のプライバシー情報
中	・社内の売上げデータ
小	・会議案内

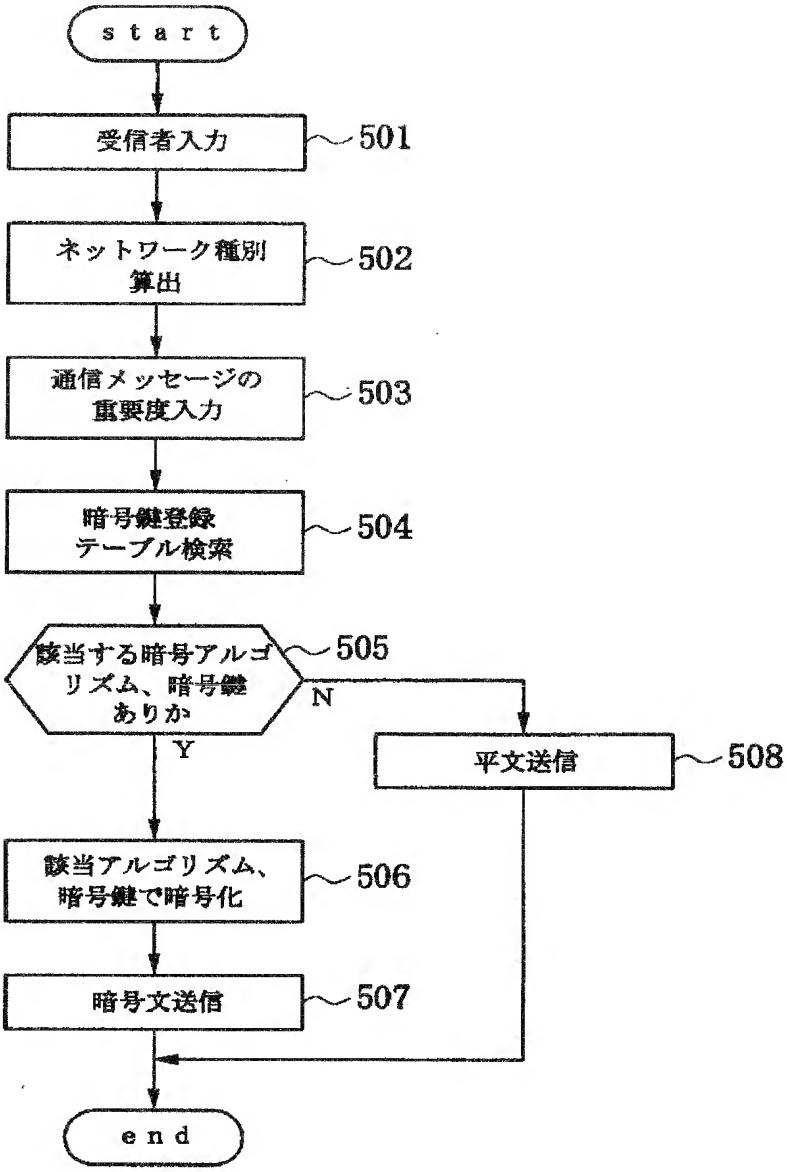
【図３】



【図４】

401 ネットワーク種別	402 メッセージ重要度	403 暗号アルゴリズム	404 鍵長（ビット）	405 暗号鍵
LAN	大	Des	40	0110・・・10
専用	大	Des	56	1100100・・・10
公衆	大	RSA	128	1111001010・・・0101
専用	中	RSA	64	011011・・・1001
インタネット	大	RSA	256	11001・・・・・・01110001
インタネット	中	RSA	128	10010100・・・1001
無線	大	RSA	256	00101・・・・・・10011110
インタネット	中	RSA	128	01100100・・・1010

【図５】


start
受信者入力
501
ネットワーク種別算出
502
通信メッセージの重要度入力
503
暗号鍵登録テーブル検索
504
該当する暗号アルゴリズム、暗号鍵ありか
505
N
Y
平文送信
508
該当アルゴリズム、暗号鍵で暗号化
506
暗号文送信
507
end